PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 6 - numero 1114 di mercoledì 03 novembre 2004

Allarme worm!

Particolarmente aggressiva la nuova variante del worm Bagle. Conosciamone le caratteristiche.

Non si placa il worm Bagle che dall'inizio dell'anno, con innumerevoli varianti, si propaga attraverso la posta elettronica e tramite le reti Peer-to-Peer.
Particolarmente aggressivo si è dimostrato l'ultimo dei prodotti "Bagle", la variante "Bagle.AT", che mette in pericolo la riservatezza dei dati custoditi sui computer infettati.
Infatti il worm termina i processi di sicurezza, dei software antivirus e di alcune altre applicazioni e, a quanto riferito da Symbolic, "installa una backdoor che ascolta sulla porta 81. Il codice di questa backdoor è cifrato tramite una password. L'autore del worm che è a conoscenza della password può collegarsi ai computer infetti ed eseguire programmi arbitrari. I computer che sono stati infettati vengono segnalati all'autore tramite indirizzi URL predefiniti."

Vediamo ora in sintesi le modalità di diffusione del worm.
Diffusione via e-mail.
Bagle.AT si propaga tramite allegato a mail infette. Il soggetto delle e-mail viene scelto tra uno dei seguenti:
Re:
Re: Hello
Re: Thank you!
Re: Thanks :)
Re: Hi
L'allegato e' composto dalle stringhe: "Price"; "price"; "Joke".
Mentre l'estesione dell'allegato è una tra le seguenti: .exe .scr .com .cpl.
Bagle.AT prima di propagarsi ricerca nel computer colpito indirizzi e-mail ai quali inviarsi.

Diffusione via peer-to-peer
Bagle.AT esegue una scansione del computer e, quando trova la cartella condivisa, vi si copia all'interno con nomi scelti in un elenco, tra i quali compaiono:
Microsoft Office 2003 Crack, Working!.exe
Microsoft Windows XP, WinXP Crack, working Keygen.exe
Porno Screensaver.scr
Serials.txt.exe
KAV 5.0
Kaspersky Antivirus 5.0
Windown Longhorn Beta Leak.exe
Opera 8 New!.exe
Adobe Photoshop 9 full.exe
Matrix 3 Revolution English Subtitles.exe
ACDSee 9.exe
